Groupe de travail Réseau
Request for Comments : 5059
RFC rendue obsolète : 2362
RFC mise à jour : 4601
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

N. Bhaskar, Arastra
A. Gall, SWITCH
J. Lingard, Arastra
S. Venaas, UNINETT
janvier 2008

Mécanisme de routeur d'amorçage (BSR) pour la diffusion groupée indépendante du protocole (PIM)

Statut du présent mémoire

Le présent document spécifie un protocole Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.
(La présente traduction incorpore les errata 1321, 1322 et 1323).

Résumé

Le présent document spécifie le mécanisme de routeur d'amorçage (BSR, *Bootstrap Router*) pour la classe des protocoles d'acheminement de diffusion groupée dans la famille de la diffusion groupée indépendante du protocole (PIM, *Protocol Independent Multicast*) qui utilise le concept de "point de rendez-vous" comme moyen pour les receveurs de découvrir les sources qui envoient à un groupe de diffusion groupée particulier. BSR est une des façons dont un routeur de diffusion groupée peut apprendre l'ensemble des transpositions de groupe à RP nécessaires pour fonctionner. Le mécanisme est dynamique, largement auto-configurant, et robuste aux défaillances de routeur.

Table des Matières

1. Introduction

Le présent document suppose une certaine familiarité avec les concepts de la diffusion groupée indépendante du protocole - mode épars (PIM-SM, *Protocol Independent Multicast - Sparse Mode*) [RFC4601] et de la diffusion groupée bidirectionnelle indépendante du protocole (BIDIR-PIM, *Bidirectional Protocol Independent Multicast*) [RFC5015], ainsi qu'avec la diffusion groupée sur IP limitée administrativement [RFC2365] et l'architecture d'adresse IPv6 calibrée [RFC4007].

Pour un fonctionnement correct, chaque routeur de diffusion groupée au sein d'un domaine PIM doit être capable de transposer une adresse particulière de groupe de diffusion groupée en le même point de rendez-vous (RP). Les spécifications de PIM ne rendent pas obligatoires l'utilisation d'un seul mécanisme pour fournir aux routeurs les informations pour effectuer cette transposition de groupe en RP.

Le présent document décrit le mécanisme de routeur d'amorçage PIM (BSR, *Bootstrap Router*). BSR est une des façons dont un routeur de diffusion groupée peut apprendre les informations requises pour effectuer la transposition de groupe en RP. Le mécanisme est dynamique, largement auto configurant, et robuste aux défaillances de routeur.

BSR a d'abord été défini dans la [RFC2362] au titre de la spécification originale de PIM-SM, qui a été rendue obsolète par la [RFC4601]. Le présent document fait une mise à jour de la spécification du mécanisme de BSR de la RFC 2362, et aussi l'étend pour traiter des frontières de région limitée administrativement et de différentes nuances des protocoles d'acheminement.

Dans le présent document, toute référence à la famille des protocoles PIM se restreint au sous ensemble des protocoles fondés sur le point de rendez-vous, à savoir PIM-SM et BIDIR-PIM, sauf mention contraire.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la RFC 2119 [RFC2119].

1.1 Fondements

Un domaine PIM est un ensemble de routeurs contigus qui tous mettent en œuvre PIM et sont configurés pour opérer au sein d'une frontière commune définie par les routeurs frontières de diffusion groupée PIM (PMBR, *PIM Multicast Border Router*). Les PMBR connectent chaque domaine PIM au reste de l'Internet.

Chaque groupe de diffusion groupée PIM doit être associé à l'adresse IP d'un point de rendez-vous (RP). Cette adresse est utilisée comme la racine d'une arborescence de distribution spécifique du groupe dont les branches s'étendent à tous les nœuds dans le domaine qui veulent recevoir le trafic envoyé au groupe. Les envoyeurs injectent les paquets dans l'arborescence de telle façon qu'ils atteignent tous les receveurs connectés. Comment cela est fait et comment les paquets sont transmis le long de l'arborescence de distribution dépend du protocole d'acheminement particulier.

Pour que tous les envoyeurs joignent tous les receveurs, il est crucial que tous les routeurs dans le domaine utilisent les mêmes transpositions d'adresses de groupe à adresses de RP.

Une exception à cela est lorsque un domaine PIM a été coupé en plusieurs régions limitées administrativement. Ce sont des régions où une frontière a été configurée de telle sorte qu'un ensemble de groupes de diffusion groupée ne sera pas transmis à travers cette frontière. Dans ce cas, tous les routeurs PIM au sein de la même région de portée doivent transposer un groupe limité particulier en le même RP au sein de cette région.

Afin de déterminer le RP pour un groupe de diffusion groupée, un routeur PIM tient une collection de transposition de groupe à RP, appelée le RP-Set. Une transposition de groupe en RP contient les éléments suivants :

- une gamme de groupes de diffusion groupée, exprimée par une adresse et une longueur de préfixe
- une priorité de RP
- une adresse de RP
- une longueur de gabarit de hachage
- un fanion SM/BIDIR.

En général, les gammes de groupe de ces transpositions de groupe à RP peuvent se chevaucher de façon arbitraire ; donc, un groupe de diffusion groupée particulier peut être couvert par plusieurs transpositions de groupe à RP. Quand c'est le cas,

le routeur choisit seulement un des RP en appliquant un algorithme déterministe afin que tous les routeurs dans le domaine fassent le même choix. Il est important de noter que cet algorithme fait partie de la spécification des protocoles individuels d'acheminement (et peut différer parmi eux) et non de la spécification de BSR. Par exemple, PIM-SM [RFC4601] définit un tel algorithme. Il utilise une fonction de hachage pour le cas où une gamme de groupes a plusieurs RP avec la même priorité. La longueur de gabarit de hachage est utilisée par cette fonction.

Ces transpositions de groupe à RP peuvent être établies de différentes façons. La solution la plus simple est que tous les routeurs dans le domaine soient configurés statiquement avec les mêmes informations. Cependant, la configuration statique ne s'adapte généralement pas bien, et, sauf quand utilisée en conjonction avec un RP à la cantonade (voir les [RFC3446] et [RFC4610]) ne s'adapte pas dynamiquement pour contourner les défaillances de routeur ou de liaison.

Le mécanisme de BSR donne un moyen de créer des transpositions viables de groupe à RP et de les distribuer rapidement à tous les routeurs PIM dans un domaine. Il est adaptable, en ce que si un RP devient inaccessible, cela va être détecté et les RP-Set vont être modifiés afin que le RP inaccessible ne soit plus utilisé.

1.2 Vue d'ensemble du protocole

Ce paragraphe donne une vue d'ensemble informelle et non définitive du mécanisme de BSR. La spécification normative commence à la Section 2.

L'idée générale derrière le mécanisme de BSR est que certains des routeurs PIM au sein d'un domaine PIM sont configurés pour être des RP potentiels pour le domaine. Il sont connus comme des candidats RP (C-RP). Un sous ensemble des C-RP va éventuellement être utilisé comme RP réels pour le domaine. De plus, certains des routeurs PIM dans le domaine sont configurés à être des candidats routeurs d'amorçage, ou candidats BSR (C-BSR). Un de ces C-BSR va être élu comme routeur d'amorçage (BSR, *Bootstrap Router*) pour le domaine, et tous les routeurs PIM dans le domaine vont apprendre le résultat de cette élection par les messages Bootstrap. Les C-RP vont alors rapporter leur candidature au BSR élu, qui choisit un sous ensemble de ces C-RP et distribue les transpositions de groupe à RP correspondantes à tous les routeurs dans le domaine avec les messages Bootstrap.

Plus en détails, le mécanisme de BSR fonctionne comme suit. Il y a quatre phases de base (bien qu'en pratique, toutes les phases puissent survenir simultanément) :

1. Élection de BSR : chaque candidat BSR génère des messages Bootstrap (BSM, *Bootstrap Message*). Chaque BSM contient un champ Priorité de BSR. Les routeurs au sein du domaine arrosent les BSM à travers le domaine. Un C-BSR qui entend un C-BSR de priorité supérieure à la sienne supprime ses envois d'autres BSM pendant un certain temps. Le seul C-BSR restant devient le BSR élu, et ses BSM informent tous les autres routeurs dans le domaine qu'il est le BSR élu.

2. Annonce de C-RP : chaque candidat RP au sein d'un domaine envoie des messages périodiques d'annonce de candidat RP (C-RP-Adv, *Candidate-RP-Advertisement*) au BSR élu. Un message C-RP-Adv inclut la priorité du C-RP annonceur, ainsi que la liste des gammes de groupes pour lesquels la candidature est annoncée. De cette façon, le BSR apprend les RP possibles qui sont actuellement actifs et accessibles.

3. Formation de RP-Set : le BSR choisit un sous ensemble des C-RP qu'il a reçus des messages C-RP-Adv pour former le RP-Set. En général, il devrait faire cela d'une façon telle que le RP-Set ne soit ni aussi grand que tous les routeurs dans le domaine ne puissent pas en être informés, ni aussi petit que la charge soit complètement concentrée sur quelques RP. Il devrait aussi tenter de produire un RP-Set qui ne change pas fréquemment.

4. Arrosage de RP-Set : dans les futurs messages Bootstrap, le BSR inclut des informations de RP-Set. Les messages Bootstrap sont arrosés à travers le domaine, ce qui assure que le RP-Set atteint rapidement tous les routeurs dans le domaine. Les BSM sont générés périodiquement pour assurer la cohérence après la restauration d'une défaillance.

Quand un routeur PIM reçoit un message Bootstrap, il ajoute les transpositions de groupe en RP qui y sont contenues à son réservoir de transpositions obtenues des autres sources (par exemple, configuration statique). Il calcule les transpositions finales des adresses de groupe en adresses de RP à partir de ce réservoir en accord avec les règles spécifiques du protocole d'acheminement particulier et utilise ces informations pour construire les arborescences de distribution de diffusion groupée.

Si un domaine PIM subit une partition, chaque zone séparée de l'ancien BSR va élire son propre BSR, qui va distribuer un RP-Set contenant des RP accessibles dans cette partition. Quand la partition se termine, une autre élection va

automatiquement se produire et seulement un des BSR va continuer d'envoyer des messages Bootstrap. Comme on s'y attend au moment d'une partition ou d'un récollement, des perturbations dans la livraison des paquets peuvent se produire. La durée de la période de perturbation va être de l'ordre du temps d'aller-retour de la région et de la valeur de BS_Timeout.

1.3 Portée administrative et BSR

Le mécanisme décrit au paragraphe précédent ne fonctionne pas quand le domaine PIM est divisé en régions limitées administrativement. Pour traiter cette situation, on utilise les modifications de protocole décrites dans ce paragraphe.

Dans la suite du présent document, on utilise le terme de zone de portée, ou simplement zone, quand on parle d'une région connectée de topologie d'une portée donnée. Pour une définition plus précise des zones de portée, voir la [RFC4007] qui développe l'idée que les zones de portée sont configurées administrativement.

La limitation administrative permet à un domaine PIM d'être divisé en plusieurs zones "admin-scope". Chaque zone "admin-scope" est un ensemble connecté convexe de routeurs PIM et est associé à un ensemble d'adresses de groupe. La frontière de la zone admin-scope est formée par des routeurs de bordure de zone (ZBR, *Zone Border Router*). Les ZBR sont configurés à ne pas transmettre de trafic pour les adresses de groupe de portée dans ou vers la zone de portée. Il est important de noter qu'une frontière de portée donnée crée toujours au moins deux zones de portée : une sur chaque côté de la frontière.

Dans IPv4, les zones limitées administrativement sont associées à un ensemble d'adresses donné par une adresse et une longueur de préfixe. Dans IPv6, les zones limitées administrativement sont associées à un ensemble d'adresses donné par une seule valeur d'identifiant de portée. L'ensemble d'adresses correspondant à une valeur d'identifiant de porté donné est défini dans la [RFC4291]. Par exemple, un identifiant de portée de 5 se transpose en les 16 gammes d'adresse IPv6 ff[0 à f]5::/16.

Il y a certaines restrictions topologiques sur les zones admin-scope. La frontière de la zone de portée doit être complète et convexe. On signifie par là qu'il ne doit pas y avoir de chemin de l'intérieur à l'extérieur de la zone de portée qui ne passe pas à travers un routeur de bordure de zone configuré, et que le chemin à capacité de diffusion groupée entre toute paire arbitraire de routeurs de diffusion groupée dans la zone de portée doit rester dans la zone.

La limitation administrative complique les BSR parce que on ne veut pas qu'un routeur PIM au sein de la zone de portée utilise un RP en dehors de la zone de portée. Donc on doit modifier le mécanisme de base pour assurer que cela n'arrive pas.

On fait cela en tenant une copie séparée du mécanisme de BSR de base, comme décrit au paragraphe précédent, au sein de chaque zone admin-scope d'un domaine PIM. Donc une élection séparée de BSR a lieu pour chaque zone admin-scope, un C-RP s'enregistre normalement auprès du BSR de chaque zone admin-scope dans laquelle il est, et chaque routeur PIM reçoit des messages Bootstrap pour chaque zone de portée dans laquelle il est. Les messages Bootstrap envoyés par le BSR pour une zone de portée particulière contiennent des informations sur les RP qui devraient être utilisés pour l'ensemble d'adresses associé à cette zone de portée.

Les messages Bootstrap sont marqués pour indiquer à quelle zone de portée ils appartiennent. Ces messages Bootstrap admin-scoped sont arrosés de la façon normale, mais ne vont pas être transmis par un ZBR à travers la frontière pour cette zone de portée.

Pour que le mécanisme de BSR fonctionne correctement avec la limitation administrative, il doit y avoir au moins un C-BSR au sein de chaque zone admin-scope, et il doit y avoir au moins un C-RP configuré à être un C-RP pour l'ensemble d'adresses de groupe associé à la zone de portée.

Même quand la limitation administrative est utilisée, une copie du mécanisme de BSR est quand même utilisée à travers le domaine PIM entier afin de distribuer les informations de RP pour les groupes qui ne sont pas limités administrativement. On appelle cette copie du mécanisme un BSR non limité. Les copies du mécanisme fonctionnant pour chaque zone admin-scope sont appelées des BSR limités.

Seuls les C-BSR et les ZBR ont besoin d'être configurés à connaître l'existence des zones de portée. Les autres routeurs, y compris les C-RP, apprennent leur existence par des messages Bootstrap.

Tous les routeurs PIM dans un domaine PIM Bootstrap où des gammes de admin-scope sont utilisées doivent être capables de recevoir des messages Bootstrap et de mémoriser le BSR gagnant et le RP-Set pour toutes les zones admin-scope qui

s'appliquent. Donc, les routeurs PIM qui mettent seulement en œuvre la RFC 2362 ou le BSR non limité (qui permet seulement un BSR par domaine) ne peuvent pas être utilisés dans les zones admin-scope d'un domaine PIM.

2. État et temporisateurs de BSR

Un routeur PIM qui met en œuvre BSR a les états suivants :

RP-Set
Par zone de portée (Z) configurée ou apprise :
À tous les routeurs :
Adresse IP courante de routeur Bootstrap
Priorité de BSR courante de routeur Bootstrap
Dernier BSM reçu du BSR courant
Temporisateur Bootstrap (BST(Z))
Par transposition de groupe en RP (M) : temporisateur de transposition de groupe en RP (GET(M,Z))

À un BSR candidat pour Z : Mon état : un de "BSR candidat", "BSR en instance", "BSR élu"

À un routeur qui n'est pas un BSR candidat pour Z :
Mon état : un de "Accepter tout", "Accepte le préféré"
Temporisateur de zone de portée (SZT(Z))

Au routeur Bootstrap courant pour Z seulement :
Transposition par groupe en C-RP (M) :
Temporisateur de groupe en C-RP (CGET(M,Z))

À un C-RP seulement : Temporisateur d'annonce de C-RP (CRPT)

3. Élection de routeur Bootstrap et distribution de RP-Set

3.1 Élection de routeur Bootstrap

Pour simplifier, les messages Bootstrap sont utilisés à la fois dans les mécanismes d'élection de BSR et de distribution de RP-Set.

Chaque message Bootstrap indique la portée à laquelle il appartient. Si le bit Zone "Admin Scope" est établi dans la première gamme de groupes dans le message Bootstrap, le message est appelé un BSM limité. Si le bit Zone "Admin Scope" n'est pas établi dans la première gamme de groupes dans le message Bootstrap, le message est appelé un BSM non limité.

Dans un BSM IPv4 limité, la portée du message est donnée par la première gamme de groupes dans le message, qui peut être toute sous-gamme de 224.0.0.0/4. Dans un BSM IPv6 limité, la portée du message est donnée par l'identifiant de portée de la première gamme de groupes dans le message, qui doit avoir une longueur de gabarit d'au moins 16. Par exemple, une gamme de groupes de ff05::/16 avec le bit Zone Admin Scope établi indique que le message Bootstrap est pour la portée qui a l'identifiant de portée 5. Si la longueur de gabarit de la première gamme de groupes dans un BSM IPv6 limité est de moins que 16, le message DOIT être éliminé et un avertissement DEVRAIT être enregistré.

L'automate à états pour les messages Bootstrap dépend de si un routeur a été ou non configuré à être un BSR candidat pour une zone de portée particulière. L'automate à états par zone de portée pour un C-BSR est donné ci-dessous, suivi par l'automate à états pour un routeur qui n'est pas configuré à être un C-BSR.

Une partie clé du mécanisme d'élection est qu'on associe une pondération à chaque BSR. Le poids d'un BSR est défini comme étant l'enchaînement dans une arithmétique de précision fixée non signée du champ Priorité de BSR provenant du message Bootstrap et de l'adresse IP du BSR provenant du message Bootstrap (avec la priorité de BSR prenant les bits de poids fort et l'adresse IP prenant les bits de moindre poids).

3.1.1 Automate à états par zone de portée de BSR candidat

Dans l'état de C-BSR

Événement	Reçoit le BSM préféré -> état C-BSR	Expiration du tempo. Bootstrap -> état P-BSR	Reçoit le BSM non-préféré du BSR élu -> état P-BSR
Action	transmet le BSM ; mémorise RP-Set ; règle tempo Bootstrap à BS_Timeout	règle tempo Bootstrap à BS_Rand_Override	transmet le BSM ; règle tempo Bootstrap à BS_Rand_Override

Dans l'état P-BSR

Événement	Reçoit le BSM préféré -> état C-BSR	Expiration du tempo. Bootstrap -> état E-BSR	Reçoit le BSM non-préféré -> état P-BSR
Action	transmet le BSM ; mémorise RP-Set ; règle tempo Bootstrap à BS_Timeout	génère le BSM règle tempo Bootstrap à BS_Period	transmet le BSM ; règle tempo Bootstrap à BS_Rand_Override

Dans l'état E-BSR

Événement	Reçoit le BSM préféré -> état C-BSR	Expiration du tempo. Bootstrap -> état E-BSR	Reçoit le BSM non-préféré -> état E-BSR
Action	transmet le BSM ; mémorise RP-Set ; règle tempo Bootstrap à BS_Timeout	génère le BSM ; règle tempo Bootstrap à BS_Period	génère le BSM ; règle tempo Bootstrap à BS_Period

Un BSR candidat peut être dans un des trois états suivants pour une zone de portée particulière :

BSR candidat (C-BSR) : le routeur est candidat pour être le BSR pour la zone de portée, mais actuellement un autre routeur est le BSR préféré.

BSR en instance (P-BSR) : le routeur est candidat pour être le BSR pour la zone de portée. Actuellement, aucun autre routeur n'est le BSR préféré, mais ce routeur n'est pas encore le BSR élu. C'est un état temporaire qui empêche des va et vient rapides du choix du BSR durant l'élection.

BSR élu (E-BSR) : le routeur est le BSR élu pour la zone de portée et il doit effectuer toutes les fonctions d'un BSR.

En plus de ces trois états, il y a un temporisateur :
Temporisateur Bootstrap (BST) - utilisé pour périmer les vieilles informations de routeur Bootstrap, et utilisé dans le processus d'élection pour mettre fin à l'état P-BSR.

L'état initial pour cette zone de portée configurée est "BSR en instance" ; le temporisateur Bootstrap est initialisé à BS_Rand_Override. C'est le cas si le routeur est un BSR candidat au démarrage, et si il est reconfiguré pour en devenir un plus tard.

3.1.2 Automate à états par zone de portée pour routeurs BSR non candidats

L'automate à états suivant est utilisé pour les zones de portée qui sont découvertes par le routeur à partir des messages Bootstrap. Un automate à états simplifié est utilisé pour les zones de portée qui sont explicitement configurées sur le routeur et pour la zone globale. Les différences sont mentionnées à la fin du paragraphe.

Dans l'état NoInfo

Événement	Réception d'un BSM -> état AP
Action	transmet le BSM ; mémorise RP-Set ; règle le temporisateur Bootstrap à BS_Timeout

Dans l'état Accepte tout

Événement	Réception d'un BSM -> état AP	Expiration du temporisateur de zone de portée -> état NoInfo
Action	transmet le BSM ; mémorise RP-Set ; règle le tempo Bootstrap à BS_Timeout	supprime l'état de zone de portée

Dans l'état Accepte le préféré			
Événement	Reçoit le BSM préféré -> état AP	Expiration du tempo. Bootstrap -> état AA	Reçoit le BSM non-préféré -> état AP
Action	transmet le BSM ; mémorise le RP-Set ; règle tempo Bootstrap à BS_Timeout	rafraîchit le RP-Set ; supprime l'état de BSR règle tempo SZT à SZ_Timeout	

Un routeur qui n'est pas un BSR candidat peut être dans un des trois états suivants :

NoInfo : le routeur n'a pas d'information sur cette zone de portée. Dans cet état, aucune information d'état n'est détenue et aucun temporisateur (qui se réfère à cette zone de portée) ne fonctionne. Idéalement, l'automate à états est seulement instancié quand le routeur reçoit un BSM limité pour une portée sur laquelle il n'a pas de connaissance a priori. Cependant, parce que le routeur passe immédiatement à l'état AA sans condition, l'état NoInfo peut être considéré comme virtuel dans un certain sens. Pour cette raison, il est omis de la description de la Section 2.

Accepte tout (AA, *Accept An*y) : le routeur ne connaît pas de BSR actif, et va accepter le premier message Bootstrap qu'il voit comme donnant l'identité du nouveau BSR et le RP-Set.

Accepte le préféré (AP, *Accept Preferred*) : le routeur connaît l'identité du BSR actuel, et il utilise le RP-Set fourni par ce BSR. Seuls les messages Bootstrap provenant de ce BSR ou d'un C-BSR avec un plus fort poids que le BSR actuel vont être acceptés.

En plus des trois états, il y a deux temporisateurs :
- o le temporisateur Bootstrap (BST) - utilisé pour périmer les vieilles informations de routeur Bootstrap.
- o le temporisateur d'expiration de zone de portée (SZT) - utilisé pour périmer la zone de portée elle-même si des messages Bootstrap spécifiant cette zone de portée cessent d'arriver.

L'état initial pour les zones de portée sur lesquelles le routeur n'a pas d'informations est "NoInfo".

L'automate à états utilisé pour les portées qui ont été configurées explicitement sur le routeur et pour la portée globale (qui existe toujours) diffère de l'automate à états ci-dessus de la façon suivante :
- o l'état "NoInfo" n'exise pas,
- o aucun SZT n'est tenu. Donc, l'événement "Expiration du temporisateur de zone de portée" n'existe pas et aucune action à l'égard de ce temporisateur n'est exécutée.

L'état initial pour pour cet automate à états est "Accepte tout".

3.1.3 Vérification du traitement du message Bootstrap

Quand un message Bootstrap est reçu, les vérifications initiales suivantes doivent être effectuées :

```
si ((DirectlyConnected(BSM.src_ip_address) == FAUX) OU
      (on n'a pas d'état Hello pour BSM.src_ip_address)) {
    éliminer en silence le message Bootstrap
  }

si (BSM.dst_ip_address == TOUS-LES-ROUTEURS-PIM) {
    si (BSM.no_forward_bit == 0) {
      si (BSM.src_ip_address != RPF_neighbor(BSM.BSR_ip_address)) {
        éliminer en silence le message Bootstrap
      }
    } autrement si ((tout BSM précédent pour cette portée a été accepté) OU
            (plus d'une BS_Period s'est écoulée depuis le démarrage)) {
      #accepte seulement un BSM no-forward si il y a rafraîchissement rapide au démarrage
      éliminer en silence le message Bootstrap
    }
  } autrement si ((la prise en charge de BSM en envoi individuel est activée) ET
          (BSM.dst_ip_address est une de mes adresses)) {
    si ((tout BSM précédent pour cette portée a été accepté) OU
       (plus d'une BS_Period s'est écoulée depuis le démarrage)) {
```

```
    #le paquet était en envoi individuel, mais ce n'était pas un rafraîchissement rapide au démarrage
    éliminer en silence le message Bootstrap
   }
  } autrement {
   éliminer en silence le message Bootstrap
  }

si (l'interface d'arrivée du message est une frontière de portée administrative pour la BSM.first_group_address) {
   éliminer en silence le message Bootstrap
  }
```

Fondamentalement, le paquet doit venir d'un voisin directement connecté pour lequel on a un état de Hello actif. Il doit avoir été envoyé au groupe TOUS-LES-ROUTEURS-PIM, et sauf si il est un BSM No-Forward (*pas de transmission*) il doit avoir été envoyé par le routeur amont correct au BSR qui a généré le message Bootstrap ; ou, si il est un BSM No-Forward, on doit avoir redémarré récemment et n'avoir pas d'état de BSR pour cette portée administrative. Aussi, si la prise en charge de BSM en envoi individuel est activée, un BSM en envoi individuel est accepté si il nous est adressé, si on a redémarré récemment, et si on n'a pas d'état de BSR pour cette portée administrative. De plus, il ne doit pas être arrivé sur une interface qui est une frontière configurée de portée administrative pour la première adresse de groupe contenue dans le message Bootstrap.

3.1.4 Événement de transition de l'automate à états

Si le message Bootstrap passe les vérifications initiales ci-dessus sans être éliminé, il peut alors causer un événement de transition d'état dans un des automates à états ci-dessus. Pour les BSR candidats et non candidats, les événements de transition suivants sont définis :

Reçoit le BSM préféré : un message Bootstrap est reçu d'un BSR qui a une pondération supérieure ou égale à celle du BSR actuel. Si un routeur est dans l'état P-BSR, il utilise alors son propre poids comme celui du BSR actuel.

Un message Bootstrap est aussi préféré si il vient du BSR actuel avec un poids inférieur à celui du BSM précédent qu'il a envoyé, pourvu que si le routeur est un BSR candidat, le BSR actuel ait encore une pondération supérieure ou égale à celle du routeur lui-même. Dans ce cas, l'état de "Priorité de BSR du routeur Bootstrap actuel" doit être mis à jour. (Pour le poids inférieur, voir le cas de BSM non préféré du BSR élu.)

Reçoit un BSM non préferé : un message Bootstrap est reçu d'un BSR autre que le BSR actuel qui a un poids inférieur à celui du BSR actuel. Si un routeur est dans l'état P-BSR, il utilise alors son propre poids comme celui du BSR actuel.

Reçoit un BSM non préferé du BSR élu : un message Bootstrap est reçu du BSR élu, mais le champ Priorité de BSR dans le message reçu a changé, de sorte que maintenant le BSR actuellement élu a un poids inférieur à celui du routeur lui-même.

Reçoit un BSM : un message Bootstrap est reçu, sans considération du poids du BSR.

En plus des transitions d'automate à états causées par la réception de messages Bootstrap, une transition d'automate à états a lieu chaque fois que le temporisateur Bootstrap ou le temporisateur d'expiration de zone de portée arrive à expiration.

3.1.5 Actions des automates à états

Les automates à états spécifient des actions qui incluent de régler le temporisateur Bootstrap et le temporisateur d'expiration de zone de portée à diverses valeurs. Ces valeurs sont définies à la Section 5.

En plus de régler et annuler les temporisateurs, les actions suivantes peuvent être déclenchées par des changements d'état dans l'automate à états :

Transmettre le BSM : un message Bootstrap en diffusion groupée avec le bit No-Forward à zéro qui passe les vérifications de traitement de message Bootstrap est transmis sur toutes les interfaces avec les voisins PIM (incluant l'interface où il est reçu) sauf lorsque cela causerait le franchissement par le BSM d'une frontière de portée administrative pour la zone de portée indiquée dans le message. Pour les détails, voir le paragraphe 3.4.

Générer un BSM : un nouveau message Bootstrap est construit par le BSR, donnant l'adresse du BSR et la priorité du BSR, et contenant le RP-Set choisi du BSR. Le message est transmis sur toutes les interfaces sur lesquelles existent des voisins PIM, sauf quand cela causerait le franchissement par le BSM d'une frontière de portée administrative pour la zone de portée indiquée dans le message.

Mémoriser le RP-Set : le routeur utilise la transposition de groupe à RP contenue dans un BSM pour mettre à jour son RP-Set local.

Cette action est sautée pour un BSM vide. Un BSM est vide si il ne contient aucune gamme de groupes, ou si il contient seulement une seule gamme de groupes et que cette gamme de groupes a le bit Zone Admin Scope établi (un BSM limité) et un compte de RP de zéro.

Si une transposition n'existe pas encore, elle est créée et le temporisateur d'expiration de transposition de groupe à RP (GET, *Group-to-RP mapping Expiry Timer*) associé est initialisé avec le temps de garde provenant du BSM.

Si une transposition existe déjà, son GET est réglé au temps de garde provenant du BSM. Si le temps de garde est zéro, la transposition est immédiatement supprimée. Noter que pour une transposition existante, la priorité de RP doit être mise à jour si elle change.

Les transpositions pour une gamme de groupes sont aussi à supprimer immédiatement si elles ne sont pas présentes dans la gamme de groupes reçue. Cela signifie que si il y a des transpositions de groupe à RP existantes pour une gamme où les RP respectifs ne sont pas dans la gamme reçue, ces transpositions doivent être supprimées.

Toutes les transpositions de RP associées à la zone de portée du BSM sont mises à jour avec la longueur du nouveau gabarit de hachage provenant du BSM reçu. Cela inclut les transpositions de RP pour toutes les gammes de groupes apprises pour cette zone, pas juste les gammes de ce BSM particulier.

De plus, le BSM entier est mémorisé pour être utilisé dans l'action Rafraîchissement de RP-Set et pour préparer un nouveau voisin PIM comme décrit ci-dessous.

Rafraîchir le RP-Set : quand le temporisateur Bootstrap expire, le routeur utilise la copie du dernier BSM qu'il a reçu pour rafraîchir son RP-Set en accord avec l'action Mémoriser le RP-Set comme si il l'avait juste reçu. Cela va augmenter les chances que les transpositions de groupe à RP n'expirent pas durant l'élection du nouveau BSR.

Supprimer l'état de BSR : quand le temporisateur Bootstrap expire, tout l'état associé au BSR courant est supprimé (adresse, priorité, BST, et dernier BSM sauvegardé ; voir la Section 2). Noter que cela n'inclut aucune transposition de groupe à RP.

Supprimer l'état de zone de portée : quand le temporisateur d'expiration de zone de portée expire, tout l'état associé à la zone de portée est supprimé (voir la Section 2).

3.2 Envoi des messages d'annonce de candidat RP

Chaque C-RP envoie périodiquement en individuel un message C-RP-Adv au BSR pour chaque zone de portée pour laquelle il a un état, pour informer le BSR de la volonté du C-RP de fonctionner comme RP. Ces messages sont envoyés avec un intervalle de C_RP_Adv_Period, sauf quand un nouveau BSR est élu ; voir ci-dessous.

Quand un nouveau BSR est élu, le C-RP DOIT envoyer un à trois messages C-RP-Adv et attendre une petite période aléatoire C_RP_Adv_Backoff avant d'envoyer chaque message. On recommande d'envoyer trois messages parce que il est important que le BSR apprenne rapidement quels RP sont actifs, et certaines pertes de paquet peuvent survenir quand un nouveau BSR est élu à cause des changements dans le réseau. Une façon de mettre cela en œuvre est de régler le CRPT à C_RP_Adv_Backoff quand le nouveau BSR est élu, ainsi que de régler un compteur à 2. Chaque fois que le CRPT expire, on envoie d'abord un message C-RP-Adv comme d'habitude. Ensuite, si le compteur n'est pas à zéro, il est décrémenté et le CRPT est de nouveau réglé à C_RP_Adv_Backoff au lieu de C_RP_Adv_Period.

Le champ Priorité dans ces messages est utilisé par le BSR pour choisir quels C-RP inclure dans le RP-Set. Noter que les plus basses valeurs de ce champ indiquent les plus fortes priorités, de sorte qu'une valeur de zéro est la plus haute priorité possible. Les C-RP devraient, par défaut, envoyer des messages C-RP-Adv avec le champ Priorité réglé à 192.

Quand un C-RP est fermé, il DEVRAIT immédiatement envoyer un message C-RP-Adv au BSR pour chaque zone de portée pour laquelle il sert actuellement de RP ; le temps de garde *(Holdtime)* dans ce message C-RP-Adv devrait être zéro. Le BSR va alors périmer immédiatement le C-RP et générer un nouveau message Bootstrap avec le temps de garde de fermeture de RP réglé à 0.

Un message C-RP-Adv porte une liste de paires de champs d'adresses de groupe et de gabarit de groupe. Cela permet au C-RP de spécifier les gammes de groupe pour lesquelles il veut être le RP. Si le C-RP devient RP, il peut appliquer cette acceptation de portée quand il reçoit des messages Register ou Join/Prune.

Un C-RP est configuré avec une liste de gammes de groupes pour lesquelles il devrait s'annoncer comme le C-RP. Un C-RP utilise l'algorithme suivant pour déterminer quelles gammes envoyer à un certain BSR.

Pour chaque gamme de groupes R dans la liste, le C-RP annonce cette gamme au BSR limité pour la plus petite portée qui "contient" R. Pour IPv6, la portée contenante est déterminée par la confrontation de l'identifiant de portée de la gamme de groupes avec la portée du BSR. Pour IPv4, c'est la plus longue correspondance de préfixe pour R, parmi les gammes de portée administrative connues. Si aucune portée ne se trouve contenir la gamme de groupes, le C-RP l'inclut dans le C-RP-Adv envoyé au BSR non limité. Si il n'est pas connu de BSR non limité, la gamme n'est incluse dans aucun C-RP-Adv.

De plus, pour chaque gamme de groupes IPv4 R dans la liste, pour chaque BSR limité dont la gamme de portées est strictement contenue dans R, le C-RP DEVRAIT par défaut annoncer la gamme de portées de ce BSR à ce BSR. Et pour chaque gamme de groupes IPv6 R dans la liste avec une longueur de préfixe < 16, le C-RP DEVRAIT par défaut annoncer chaque sous gamme de longueur de préfixe 16 au BSR limité avec l'identifiant de portée correspondant. Une mise en œuvre PEUT fournir une option de configuration pour empêcher le comportement décrit dans ce paragraphe, mais cette option DEVRAIT être désactivée par défaut.

Pour IPv6, la longueur de gabarit de toutes les gammes de groupes incluse dans le message C-RP-Adv envoyé à un BSR limité DOIT être ≥ 16.

Si l'algorithme ci-dessus détermine qu'il n'y a pas de gammes de groupes à annoncer au BSR pour une zone de portée particulière, un message C-RP-Adv NE DOIT PAS être envoyé à ce BSR. Un C-RP NE DOIT PAS envoyer de message C-RP-Adv sans gammes de groupes dedans.

Si le même routeur est le BSR pour plus d'une zone de portée, les messages C-RP-Adv pour ces zones de portée PEUVENT être combinés dans un seul message.

Si le C-RP est un ZBR pour une zone de portée administrative, alors le bit Admin Scope Zone DOIT être établi dans les messages C-RP-Adv qu'il envoie pour cette zone de portée ; autrement ce bit NE DOIT PAS être établi. Cette information est actuellement seulement utilisée pour des besoins de journal d'événements par le BSR, mais pourrait permettre de futures extensions du protocole.

3.3 Création de RP-Set au BSR

À réception d'un message C-RP-Adv, le routeur doit décider si il accepte ou non chacune des gammes de groupes incluses dans le message. Pour chaque gamme de groupes du message, le routeur vérifie si il est le BSR élu pour toute zone de portée qui contient la gamme de groupes, ou si il est élu comme BSR non limité. Si il l'est, la gamme de groupes est acceptée ; sinon, la gamme de groupes est ignorée.

Pour des raisons de sécurité, on recommande que les mises en œuvre aient un moyen de restreindre les adresses IP dont le BSR accepte les messages C-RP-Adv, par exemple, avec les listes d'accès. En utilisant un BSR limité, il peut aussi être utile de spécifier quelles gammes de groupes devraient être acceptées.

Si la gamme de groupes est acceptée, une transposition de groupe à C-RP est créée pour cette gamme de groupes et l'adresse de RP provenant du message C-RP-Adv.

Si la transposition ne fait pas déjà partie du C-RP-Set, elle est ajoutée au C-RP-Set et le temporisateur d'expiration de transposition de groupe à C-RP (CGET) associé est initialisé au temps de garde provenant du message C-RP-Adv. Sa priorité est réglée à la priorité provenant du message C-RP-Adv.

Si la transposition fait déjà partie du C-RP-Set, il est mis à jour avec la priorité provenant du message C-RP-Adv., et son CGET associé est remis au temps de garde provenant du message C-RP-Adv. Si le temps de garde est zéro, la transposition est immédiatement supprimée du C-RP-Set.

La longueur du gabarit de hachage est une propriété globale du BSR et est donc la même pour toutes les transpositions gérées par le BSR.

Pour la compatibilité avec les précédentes versions de la spécification de BSR, un message C-RP-Adv sans gamme de groupes DEVRAIT être traité comme si il contenait la seule gamme de groupes ff00::/8 ou 224.0.0.0/4. Donc, en accord avec la règle ci-dessus, cette gamme de groupes va être acceptée si et seulement si le routeur est élu comme BSR non limité.

Quand un CGET expire, la transposition de groupe à C-RP correspondante est supprimée du C-RP-Set.

Le BSR construit le RP-Set à partir du C-RP-Set. Il peut appliquer une politique locale pour limiter le nombre de RP candidats inclus dans le RP-Set. Le BSR peut outrepasser la gamme indiquée dans un message C-RP-Adv sauf si le champ "Priorité" dans le message C-RP-Adv est inférieur à 128.

Si le BSR apprend des RP candidats de BIDIR et de PIM-SM pour la même gamme de groupes, il DOIT seulement inclure les RP pour un des protocoles dans les BSM. Le comportement par défaut DEVRAIT être de préférer BIDIR.

Pour l'inclusion dans un BSM, le RP-Set est subdivisé en ensembles de {gamme de groupes, compte de RP, adresses de RP}. Pour chaque adresse de RP, le champ "RP-Holdtime" est réglé au temps de garde provenant du C-RP-Set, sous réserve de la contrainte qu'il DOIT être plus grand que BS_Period et DEVRAIT être plus grand que 2,5 fois BS_Period pour permettre que des messages Bootstrap soient perdus. Si des temps de garde provenant du C-RP-Sets ne satisfont pas cette contrainte, le BSR DOIT remplacer ces temps de garde par une valeur satisfaisant la contrainte. Une exception est le temps de garde de zéro, qui est utilisée pour supprimer immédiatement des transpositions.

Le format du message Bootstrap permet la "fragmentation sémantique", si la longueur du message Bootstrap d'origine excède les limites maximum de paquet. Cependant, pour réduire la fragmentation sémantique requise, on recommande de ne pas configurer un grand nombre de routeurs comme C-RP.

En général, les BSM sont générés à des intervalles réguliers en accord avec le temporisateur BS_Period. On recommande qu'un BSM soit aussi généré chaque fois que change le RP-Set à annoncer dans les BSM. Cela va généralement se produire quand on reçoit des annonces de C-RP d'un nouveau C-RP, ou quand un C-RP est fermé (annonce de C-RP avec un temps de garde de zéro). Il DOIT cependant y avoir un minimum de BS_Min_Interval entre chaque envoi d'un BSM. En particulier, quand un nouveau BSR est élu, il va d'abord envoyer un BSM (qui va probablement être vide car il n'a pas encore reçu d'annnonce de C-RP) et ensuite attendre au moins BS_Min_Interval avant d'en envoyer un nouveau. Durant ce temps, il est probable qu'il aura reçu des annonces de C-RP de tous les C-RP utilisables (car on dit qu'un C-RP devrait envoyer une ou plusieurs annonces avec de petits délais aléatoires de C_RP_Adv_Backoff quand un nouveau BSR est élu). Pour ce cas en particulier, où les routeurs peuvent ne pas avoir de RP-Set utilisable, on recommande de générer un BSM aussitôt que BS_Min_Interval s'est écoulé. On suggère cependant qu'un BSR puisse faire cela en général. Une façon de mettre cela en œuvre est de diminuer le temporisateur Bootstrap à BS_Min_Interval chaque fois que le RP-Set change, et de ne pas changer le temporisateur si il est inférieur ou égal à BS_Min_Interval.

Un BSR génère des BSM limités séparés pour chaque zone de portée pour laquelle il est le BSR élu, ainsi que des BSM non limités si il est le BSR non limité élu.

Chaque transposition de groupe à C-RP est incluse dans précisément un de ces BSM -- à savoir, le BSM limité pour la portée la plus étroite contenant la gamme de groupes de la transposition, si il en est, ou autrement le BSM non limité.

Un BSM limité DOIT avoir au moins une gamme de groupes, et la première gamme de groupes dans un BSM limité DOIT avoir le bit Admin Scope Zone établi. Cette gamme de groupes identifie la portée du BSM. Dans un BSM IPv4 limité, la première gamme de groupes est la gamme correspondant à la portée du BSM. Dans un BSM IPv6 limité, la première gamme de groupes peut être toute gamme de groupes sous réserve de la condition générale que toutes les gammes de groupes dans un tel BSM DOIVENT avoir une longueur de gabarit d'au moins 16 et DOIVENT avoir le même identifiant de portée que la portée du BSM.

À part l'identification de la portée, la première gamme de groupes dans un BSM limité est traitée comme toute autre gamme à l'égard des transpositions de RP. C'est-à-dire que toutes les transpositions dans le RP-Set pour cette gamme de groupes, si

il en est, doivent être incluses dans cette première gamme de groupes dans le BSM. Après cette gamme de groupes, les autres gammes de groupes dans cette portée (pour laquelle il y a les transpositions de RP) apparaissent dans n'importe quel ordre.

Le bit Admin Scope Zone de toutes les gammes de groupes autres que la première DEVRAIT être réglé à 0 à l'émission, et DOIT être ignoré à réception.

Quand un BSR élu est fermé, il devrait immédiatement générer un message Bootstrap faisant la liste de ses RP-Set actuels, mais avec le champ Priorité de BSR réglé à la plus faible valeur de priorité possible. Cela va causer plus rapidement l'élection d'un nouveau BSR.

3.4 Transmissiion des messages Bootstrap

Généralement, les messages Bootstrap sont générés au BSR, et sont transmis bond par bond par des routeurs intermédiaires si ils passent les vérifications de traitement de message Bootstrap. Il ya deux exceptions à cela. Une est qu'un message Bootstrap n'est pas transmis si son bit No-Forward est établi ; voir le paragraphe 3.5.1. L'autre est que les BSM en envoi individuel (voir le paragraphe 3.5.2) ne sont généralement pas transmis. Les mises en œuvre PEUVENT cependant à leur discrétion choisir de renvoyer un BSM No-Forward ou en envoi individuel dans un BSM en diffusion groupée, qui DOIT avoir le bit No-Forward à zéro. Il est essentiel que le bit No-Forward soit à zéro, car aucune vérification de la transmission sur le chemin inverse (RPF, *Reverse Path Forwarding*) n'est effectuée par le receveur quand il est établi.

Par transmission bond par bond, on veut dire que le message Bootstrap lui-même est transmis, pas le paquet IP entier. Chaque bond construit un paquet IP pour chacune des interfaces à partir desquelles le BSM est à transmettre ; chaque paquet contient le BSM entier reçu.

Quand un message Bootstrap est transmis, il l'est sur chaque interface capable de diffusion groupée qu'ont les voisins PIM (y compris celle sur laquelle le message a été reçu). La seule exception à cela est si l'interface est une frontière de portée administrative pour la zone de portée administrative indiquée dans la première gamme de groupes dans le paquet du message Bootstrap.

À titre d'optimisation, un routeur PEUT choisir de ne pas transmettre un BSM sur l'interface où le message a été reçu si cette interface est en point à point. Sur les interfaces avec plusieurs voisins PIM, un routeur DEVRAIT transmettre un BSM accepté sur l'interface où ce BSM a été reçu, mais si le nombre de voisins PIM sur cette interface est grand, il PEUT retarder la transmission d'un BSM sur cette interface d'un petit intervalle aléatoire pour empêcher une explosion de messages. Une option de configuration PEUT être fournie pour désactiver la transmission sur l'interface d'où un message a été reçu, mais on recommande que le comportement par défaut soit de transmettre sur cette interface.

Raison : un BSM a besoin d'être transmis sur l'interface d'où le message a été reçu (en plus des autres interfaces) parce que les routeurs sur un LAN peuvent ne pas avoir des informations d'acheminement cohérentes. Si trois routeurs sur un LAN sont A, B, et C, et qu'au routeur B RPF(BSR)==A et au routeur C RPF(BSR)==B, alors le routeur A transmet à l'origine le BSM sur le LAN, mais le routeur C va seulement l'accepter quand le routeur B retransmet le message sur le LAN. Si la configuration de protocole d'acheminement sous-jacente garantit que les routeurs ont des informations d'acheminement cohérentes, alors la transmission sur l'interface entrante peut être désactivée en toute sécurité.

Un ZBR contraint tous les BSM qui sont de portée égale ou inférieure à la limite configurée. C'est-à-dire, les BSM ne sont pas acceptés, générés, ou transmis sur les interfaces sur lesquelles la limite est configurée. Pour IPv6, la vérification est une comparaison entre la portée de la première gamme dans le BSM limité et la portée de la limite configurée. Pour IPv4, la première gamme dans le BSM limité est vérifiée pour voir si elle est contenue dans, ou est la même que, la gamme de la limite configurée.

3.5 Messages Bootstrap aux routeurs nouveaux et en réamorçage

Quand un message Hello est reçu d'un nouveau voisin, ou quand un message Hello avec un nouveau GenID est reçu d'un voisin existanr, un seul routeur sur le LAN envoie une copie mémorisée du message Bootstrap pour chaque zone de portée administrative au routeur nouveau ou qui se réamorce. Cela permet aux routeurs nouveaux ou qui se réamorcent d'apprendre rapidement le RP-Set.

Ce message DEVRAIT être envoyé comme message Bootstrap No-Forward (voir au paragraphe 3.5.1). Pour la rétro compatibilité, ce message PEUT à la place ou en plus être envoyé comme message Bootstrap en envoi individuel (voir au paragraphe 3.5.2). Ces messages DOIVENT seulement être acceptés au démarrage (voir au paragraphe 3.5.3).

Le routeur qui fait cela est le routeur désigné (DR, *Designated Router*) sur le LAN, ou, si le routeur nouveau ou qui réamorce est le DR, celui qui serait le DR si le routeur nouveau ou qui réamorce était exclu du processus d'élection de DR.

Avant d'envoyer un message Bootstrap de cette manière, le routeur doit attentre d'avoir envoyé un message Hello déclenché sur cette interface ; autrement, le nouveau voisin va éliminer le message Bootstrap.

3.5.1 Messages Bootstrap No-Forward

Un message Bootstrap No-Forward, est un message Bootstrap qui a le bit No-Forward établi. Toutes les mises en œuvre DEVRAIENT prendre en charge l'envoi de messages Bootstrap No-Forward, et DEVRAIENT aussi les accepter. La vérification de RPF NE DOIT PAS être effectuée dans la vérification de traitement de BSM pour un BSM No-Forward (voir au paragraphe 3.1.3). Les messages ont les mêmes adresses de source et de destination que les messages Bootstrap en diffusion groupée habituels.

3.5.2 Messages Bootstrap Unicasting

Pour la rétro compatibilité, les mises en œuvre PEUVENT prendre en charge les messages Bootstrap en envoi individuel. On DEVRAIT pouvoir configurer si les messages Bootstrap sont en envoi individuel au lieu de ou en plus des messages Bootstrap No-Forward, et aussi si on accepte de tels messages. Ce message est en envoi individuel au voisin.

3.6 Réception et utilisation de RP-Set

Le RP-Set tenu par BSR est utilisé par les protocoles d'acheminement de diffusion groupée fondés sur le RP comme PIM-SM et BIDIR-PIM. Ces protocoles peuvent aissi obtenir des RP-Set d'autres sources. Comment les transpositions finales de groupe à RP sont obtenues de ces RP-Set ne fait pas partie de la spécification du BSR. En général, les protocoles d'acheminement ont besoin de recalculer les transpositions quand un de leurs RP-Set change. Comment un tel changement est signalé au protocole d'acheminement sort aussi du domaine d'application de la présente spécification.

Certaines transpositions de groupe à RP dans le RP-Set indiquent des gammes de groupes pour lesquelles PIM-SM devrait être utilisé ; d'autres indiquent des gammes de groupes à utiliser avec BIDIR-PIM. Les routeurs qui ne prennent en charge qu'un seul de ces protocoles NE DOIVENT PAS ignorer les gammes indiquées comme étant pour l'autre protocole. Ils NE DOIVENT PAS les traiter comme étant pour le protocole qu'ils prennent en charge.

Si une transposition ne fait pas encore partie du RP-Set, elle est ajoutée au RP-Set et le temporisateur d'expiration de transposition de groupe à RP (GET) associé est initialisé au temps de garde provenant du message Bootstrap. Sa priorité est réglée à la priorité provenant du message Bootstrap.

Si une transposition fait déjà partie du RP-Set, elle est mise à jour avec la priorité provenant du message Bootstrap et son GET associé est remis au temps de garde provenant du message Bootstrap. Si le temps de garde est zéro, la transposition est immédiatement supprimée du RP-Set.

4. Formats de message

Les messages de BSR sont des messages PIM, comme défini dans la [RFC4601]. Les valeurs du champ Type de message PIM pour les messages de BSR sont :

4 Bootstrap *(amorçage)*
8 Candidate-RP-Advertisement *(annonce de candidat point de rendez-vous)*

Comme avec tous les autres messages de contrôle PIM, les messages de BSR ont le numéro de protocole IP 103.

Les messages Candidate-RP-Advertisement sont en envoi individuel à un BSR. Généralement, les messages Bootstrap sont en diffusion groupée avec un TTL de 1 au groupe ALL-PIM-ROUTERS *(tous les routeurs PIM)*, mais dans certaines

circonstances (décrites au paragraphe 3.5.2) les messages Bootstrap peuvent être en envoi individuel à un voisin PIM spécifique.

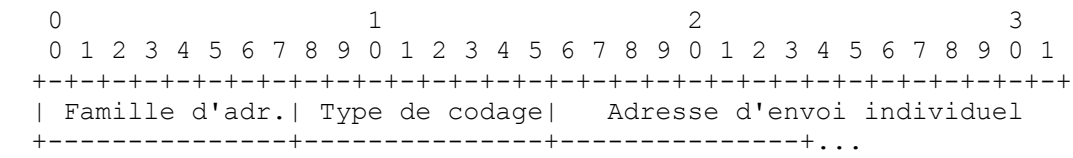
L'adresse IP de source utilisée pour les messages Candidate-RP-Advertisement est une adresse accessible sur l'ensemble du domaine. L'adresse IP de source utilisée pour les messages Bootstrap (sans considération de si ils sont générés ou transmis) est l'adresse de liaison locale de l'interface sur laquelle le message est envoyé (c'est-à-dire, la même adresse de source que celle que le routeur utilise pour les messages Hello qu'il envoie sur cette interface).

Le groupe IPv4 ALL-PIM-ROUTERS est 224.0.0.13. Le groupe IPv6 ALL-PIM-ROUTERS est ff02::d.

Dans cette Section, on utilise les termes suivants définis dans la spécification PIM-SM [RFC4601] :
- o format codé en envoi individuel
- o format codé de diffusion groupée

On les répète ici pour faciliter la lisibilité.

Adresse codée en envoi individuel ; elle prend le format suivant :

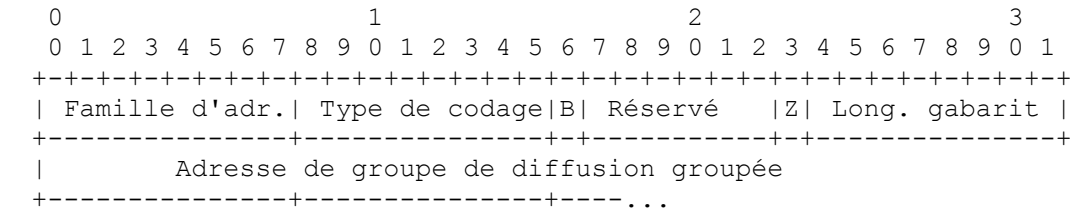


Famille d'adresses : la famille d'adresses PIM du champ "Adresse d'envoi individuel" de cette adresse. Les valeurs de 0 à 127 sont allouées par l'IANA pour les familles d'adresses Internet dans [IANA]. Les valeurs de 128 à 250 sont réservées pour être allouées par l'IANA pour des familles d'adresses spécifiques de PIM. Les valeurs de 251 à 255 sont destinées à une utilisation privée. Comme il n'y a pas d'autorité d'allocation pour cet espace, on devrait s'attendre à des collisions.

Type de codage : celui utilisé dans une famille d'adresses spécifique. La valeur "0" est réservée pour ce champ, et représente le codage natif de la famille d'adresses.

Adresse d'envoi individuel : adresse d'envoi individuel telle que représentée par la famille d'adresses et le type de codage.

Les adresses codées en diffusion groupée ont le format suivant :



Famille d'adresses : décrite plus haut

Type de codage : décrit plus haut

PIM [B]idirectionnel : indique que la gamme de groupes utilise PIM bidirectionnel [RFC5015]. Pour PIM-SM comme défini dans la présente spécification, ce bit DOIT être zéro.

Réservé : zéro à l'émission, ignoré à réception.

[Z]one de portée administrative : Quand il est établi, ce bit indique que cette gamme de groupes est une gamme limitée administrativement.

Longueur de gabarit : c'est un champ de 8 bits. La valeur est le nombre de bits un contigus qui sont justifiés à gauche et utilisés comme gabarit ; quand ils sont combinés à l'adresse de groupe, elle décrit une gamme de groupes. Elle est inférieure ou égale à la longueur d'adresse en bits pour la famille d'adresses et le type de codage donnés. Si le message est envoyé pour un seul groupe, la longueur de gabarit doit alors être égale à la longueur d'adresse en bits pour la

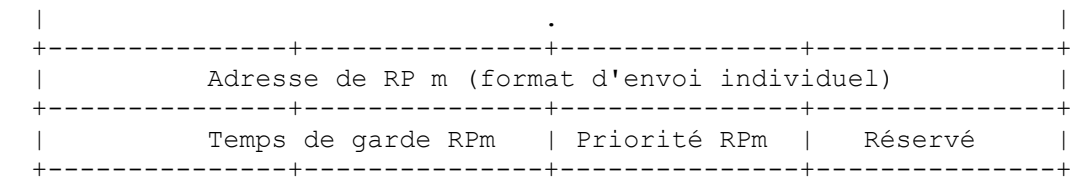
famille d'adresses et le type de codage donnés (par exemple, 32 pour le codage IPv4 natif, 128 pour le codage IPv6 natif).

Adresse de groupe de diffusion groupée : contient l'adresse du groupe.

4.1 Format du message Bootstrap

Un message Bootstrap peut être divisé en plusieurs "fragments sémantiques" si le datagramme IP résultant excèderait les limites maximum de taille de paquet. Fondamentalement, un seul message Bootstrap peut être envoyé en plusieurs fragments sémantiques (chacun dans un datagramme IP séparé) pour autant que les étiquettes de fragment de tous les fragments sémantiques composant le message soient les mêmes. Le format d'un seul message non fragmenté est le même que celui utilisé pour les fragments sémantiques.

Le format d'un seul "fragment" est donné ci-dessous :



Version PIM, Réservé, Somme de contrôle sont décrits dans la [RFC4601].

Type : Type de message PIM. La valeur est 4 pour un message Bootstrap.

Bit [N]o-Forward : quand il est établi, ce bit signifie que le fragment de message Bootstrap n'est pas à transmettre.

Étiquette de fragment : nombre aléatoire, pour distinguer les fragments appartenant à différents messages Bootstrap ; les fragments appartenant au même message Bootstrap portent la même "étiquette de fragment".

Longueur de gabarit de hachage : longueur (en bits) du gabarit à utiliser dans la fonction de hachage. Pour IPv4, on recommande une valeur de 30. Pour IPv6, on recommande une valeur de 126.

Priorité de BSR : contient la valeur de priorité de BSR du BSR inclus. Ce champ est considéré comme un octet de poids fort pour la comparaison des adresses de BSR. Les BSR devraient par défaut régler ce champ à 64. Noter que pour des raisons historiques, la plus forte priorité de BSR est 255 (la plus forte est la meilleure) tandis que la plus forte priorité de RP (voir ci-dessous) est 0 (la plus basse est la meilleure).

Adresse de BSR : adresse du routeur Bootstrap pour le domaine. Le format de cette adresse est donné dans le format d'adresse d'envoi individuel (voir la Section 4 ci-dessus).

Adresse de groupe 1 à n : les gammes de groupes (adresse et gabarit) auxquelles les RP candidats sont associés. Le format est décrit dans la [RFC4601]. Dans un fragment contenant des gammes admin-scope, la première gamme de groupes dans le fragment DOIT satisfaire les conditions suivantes :

- o elle DOIT avoir le bit Admin Scope Zone établi ;
- o pour IPv4, elle DOIT être la gamme de groupes pour la gamme admin-scope entière (c'est exigé même si il n'y a pas de RP dans le RP-Set pour la gamme admin-scope entière -- dans ce cas, les sous-gammes pour le RP-Set sont spécifiées plus tard dans le fragment avec leurs RP) ;
- o pour IPv6, la longueur de gabarit DOIT être au moins 16 et avoir l'identifiant de portée de la gamme admin-scope.

Compte RP 1 à n : nombre d'adresses de RP candidats incluses dans le message Bootstrap entier pour la gamme de groupes correspondante. Un routeur ne remplace pas son vieux RP-Set pour une gamme de groupes donnée jusqu'à ce qu'il reçoive des adresses de "RP-Count" pour cette gamme ; les adresses pourraient être portées sur plusieurs fragments. Si seulement une partie du RP-Set pour une certaine gamme de groupes a été reçue, le routeur l'élimine dans mettre à jour le RP-Set de cette gamme de groupes spécifique.

Frag RP Cnt 1 à n : nombre d'adresses de RP candidats incluses dans ce fragment du message Bootstrap, pour la gamme de groupes correspondante. Le champ "Frag RP Cnt" facilite l'analyse du RP-Set pour une certaine gamme de groupes, quand il est porté sur plus d'un fragment.

Adresse de RP 1 à m : adresse des RP candidats, pour la gamme de groupes correspondante. Le format de ces adresses est donné dans le format d'adresse d'envoi individuel (voir la Section 4 ci-dessus).

Temps de garde de RP 1 à m : temps de garde (en secondes) pour le RP correspondant. Ce champ est copié du champ "Temps de garde du RP associé mémorisé au BSR.

Priorité de RP 1 à m : "priorité" du RP correspondant et de l'adresse de diffusion groupée. Ce champ est copié du champ "Priorité" mémorisé au BSR quand il reçoit un message C-RP-Adv. La plus forte priorité est "0" (c'est-à-dire, à la différence de la priorité de BSR, plus la valeur du champ "Priorité" est faible, meilleure elle est). Noter que la priorité est par RP et par adresse de diffusion groupée.

Au sein d'un message Bootstrap, l'adresse de BSR, toutes les adresses de diffusion groupé, et toutes les adresses de RP DOIVENT être de la même famille d'adresses. De plus, la famille d'adresses des champs dans le message DOIT être la

même que les adresses IP de source et de destination du paquet. Cela permet une souplesse maximum de mise en œuvre pour les routeurs IPv4/IPv6 à double pile.

4.1.1 Fragmentation sémantique des BSM

Les messages Bootstrap peuvent être partagés sur plusieurs fragments de messages Bootstrap (BSMF, *Bootstrap Message Fragment*) PIM ; c'est appelé une fragmentation sémantique. Chacun d'eux doit avoir le format ci-dessus. Tous les fragments d'un message Bootstrap donné DOIVENT avoir des valeurs identiques des champs Type, Bit No-Forward, Étiquette de fragment, Longueur de gabarit de hachage, Priorité de BSR, et Adresse de BSR. C'est-à-dire que seules les transpositions de groupe à RP peuvent différer entre les fragments.

Ceci est utile si le BSM excèderait autrement la MTU de la liaison sur laquelle le message va être transmis. Si on s'appuie seulement sur la fragmentation IP, on perdrait le message entier si un seul fragment était perdu. En utilisant la fragmentation sémantique, un seul fragment IP perdu va seulement causer la perte du fragment sémantique dont le fragment IP faisait partie. Comme décrit ci-dessous, un routeur a seulement besoin de recevoir tous les RP pour une gamme de groupes spécifique pour mettre à jour cette gamme. Cela signifie que la perte d'un fragment sémantique, due à la perte d'un fragment IP, affecte seulement les gammes de groupes pour lesquelles le fragment sémantique perdu contient des informations.

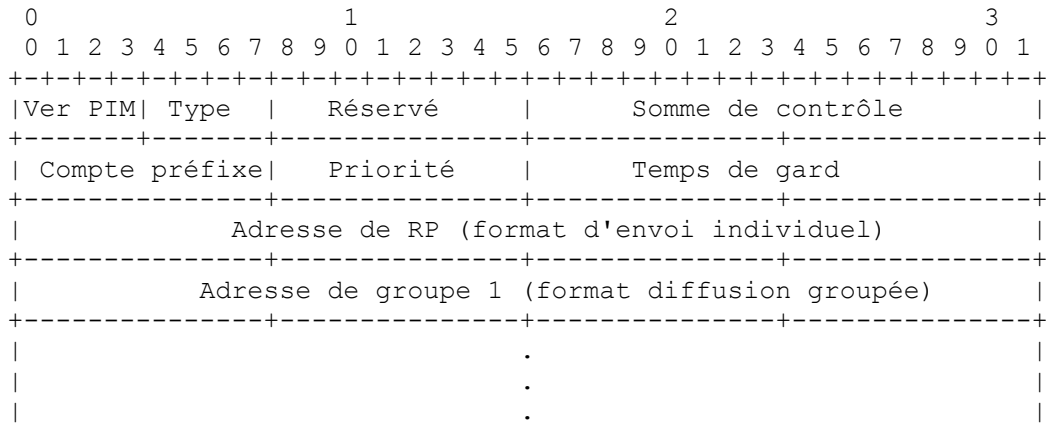
Si le BSR peut partager le BSM afin que chaque gamme de groupes (et toutes ses informations de RP) puisse tenir entièrement dans un BSMF, il devrait alors le faire. Si un BSMF est perdu, on va conserver l'état provenant du BSM précédent pour la gammes de groupes du BSMF manquant. Chaque fragment qui arrive va mettre à jour les informations de RP pour les gammes de groupes contenues dans ce fragment, et les nouvelles transpositions de groupe à RP pour elles peuvent être utilisées immédiatement. Les informations provenant du fragment manquant vont être obtenues quand le prochain BSM sera transmis.

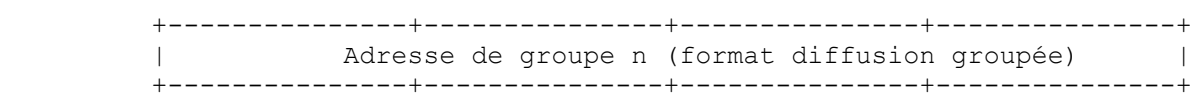
Si la liste des RP pour une seule gamme de groupes est longue, on peut partager les informations sur plusieurs BSMF pour éviter la fragmentation IP. Dans ce cas, tous les BSMF composant l'information pour cette gamme de groupes doivent être reçus avant que la transposition de groupe en RP utilisée puisse être modifiée. C'est l'objet du champ Compte de RP -- un routeur qui reçoit des BSMF provenant du même BSM (c'est-à-dire, qui ont la même étiquette de fragment) doit attendre jusqu'à ce que les BSMF fournissant les RP de compte de RP pour cette gamme de groupes aient été reçus avant que la nouvelle transposition de groupe en RP puisse être utilisée pour cette gamme de groupes. Si un seul BSMF pour une grande gamme de groupes est perdue, alors cette gamme de groupes entière va devoir attendre que le prochain BSM soit généré. Donc, dans ce cas, l'avantage de l'utilisation de la fragmentation sémantique est douteux.

On examine ensuite comment un BSR va supprimer des gammes de groupes. Un routeur qui reçoit un ensemble de BSMF ne peut pas dire si une gamme de groupes manque. Si il a vu une gamme de groupes avant, il doit supposer que cette gamme de groupes existe encore, et que le BSMF qui décrit cette gamme de groupes a été perdu. Le routeur devrait conserver cette information pendant BS_Timeout. Donc, pour qu'un BSR suppime une gamme de groupes, il devrait inclure cette gamme de groupes, mais avec un compte de RP de zéro, et il devrait renvoyer cette information dans chaque BSM pendant BS_Timeout.

4.2 Format du message Candidate-RP-Advertisement

Les messages Candidate-RP-Advertisement sont périodiquement en envoi individuel des C-RP au BSR.





Version PIM, Réservé, Somme de contrôle sont décrits dans la [RFC4601].

Type : Type de message PIM. La valeur est 8 pour un message Candidate-RP-Advertisement.

Compte de préfixe : nombre d'adresses de diffusion groupée incluses dans le message ; indique la gamme de groupes pour laquelle le C-RP annonce. Les C-RP NE DOIVENT PAS envoyer de messages C-RP-Adv avec un compte de préfixe de "0".

Priorité : priorité du RP inclus, pour l'adresse de diffusion groupée correspondante (si il en est). La plus forte priorité est "0" (c'est-à-dire, moins la valeur du champ "Priorité" est élevée, plus forte est la priorité). Ce champ est mémorisé au BSR à réception avec l'adresse du RP et l'adresse de diffusion groupée correspondante.

Temps de garde : durée (en secondes) pendant laquelle l'annonce est valide. Ce champ permet que des annonces soient périmées. Ce champ devrait être réglé à 2,5 fois C_RP_Adv_Period.

Adresse de RP : adresse de l'interface pour s'annoncer comme RP candidat. Le format de cette adresse est donné dans le format d'adresse d'envoi individuel (voir la Section 4 ci-dessus).

Adresse de diffusion groupée 1 à n : gammes de groupes pour lesquelles le C-RP annonce. Le format est décrit comme adresse de diffusion groupée dans la [RFC4601].

Dans un message Candidate-RP-Advertisement, l'adresse de RP et toutes les adresses de diffusion groupée DOIVENT être de la même famille d'adresses. De plus, la famille d'adresse des champs dans le message DOIT être la même que les adresses IP de source et de destination du paquet. Cela permet une souplesse maximum de mise en œuvre pour les routeurs IPv4/IPv6 à double pile.

5. Temporisateurs et valeurs de temporisation

Nom du temporisateur : Temporisateur Bootstrap (BST(Z))

Nom de valeur	**Valeur**	**Explication**
BS_Period	par défaut 60 s	Intervalle périodique auquel les BSM sont normalement générés
BS_Timeout	par défaut 130 s	Intervalle après lequel un BSR est périmé si aucun BSM n'est reçu de ce BSR
BS_Min_Interval	par défaut 10 s	Intervalle minimum auquel les BSM peuvent être générés
BS_Rand_Override	voir ci-dessous	Intervalle aléatoire utilisé pour réduire les frais généraux de message de contrôle durant l'élection de BSR

Noter que BS_Timeout DOIT être supérieur à BS_Period, même si leurs valeurs ne sont pas les valeurs par défaut. On recommande que BS_Timeout soit réglé à 2 fois BS_Period plus 10 secondes.

BS_Rand_Override est calculé en utilisant le pseudo code suivant, dans lequel toutes les valeurs sont en unités de secondes. Les valeurs de BS_Rand_Override générées par ce pseudo code sont entre 5 et 23 secondes, avec de plus petites valeurs générées si le C-BSR a une pondération Bootstrap élevée, et de plus grandes valeurs générées si le C-BSR a une faible pondération Bootstrap.

```
BS_Rand_Override = 5 + priorityDelay + addrDelay
```

où priorityDelay est donnée par :

```
priorityDelay = 2 * log_2(1 + bestPriority - myPriority)
```

et addrDelay est donné par ce qui suit pour IPv4 :

```
si (bestPriority == myPriority) {
  addrDelay = log_2(1 + bestAddr - myAddr) / 16
```

```
} autrement {
  addrDelay = 2 - (myAddr / 2^31)
}
```

et addrDelay est donné par ce qui suit pour IPv6 :

```
si (bestPriority == myPriority) {
  addrDelay = log_2(1 + bestAddr - myAddr) / 64
} autrement {
  addrDelay = 2 - (myAddr / 2^127)
}
```

bestPriority est donné par :

```
    bestPriority = max(storedPriority, myPriority)
```

et bestAddr est donné par :

```
    bestAddr = max(storedAddr, myAddr)
```

et myAddr est l'adresse du BSR candidat, storedAddr est l'adresse de BSR mémorisée, myPriority est la priorité configurée du BSR candidat, et storedPriority est la priorité mémorisée du BSR.

Nom du temporisateur : Temporisateur d'expiration de zone de portée (SZT(Z))

Nom de valeur	**Valeur**	**Explication**
SZ_Timeout	Par défaut : 1300 s	Intervalle après lequel une zone de portée est périmée si aucun BSM n'est reçu pour cette zone de portée

Noter que SZ_Timeout DOIT être supérieur à BS_Timeout, même si leurs valeurs sont changées par rapport aux valeurs par défaut. On recommande que SZ_Timeout soit réglé à 10 fois BS_Timeout.

Nom du temporisateur : Temporisateur d'expiration de transposition de groupe à C-RP (CGET(M,Z))

Nom de valeur	**Valeur**	**Explication**
C-RP Mapping Timeout	d'après le message	Temps de garde provenant du message C-RP-Adv

Nom du temporisateur : Temporisateur d'expiration de transposition de groupe à RP (GET(M,Z))

Nom de valeur	**Valeur**	**Explication**
RP Mapping Timeout	d'après le message	Temps de garde provenant du BSM

Nom du temporisateur : C-RP Advertisement Timer (CRPT)

Nom de valeur	**Valeur**	**Explication**
C_RP_Adv_Period	par défaut : 60 s	Intervalle périodique avec lequel les messages C-RP-Adv sont envoyés à un BSR
C_RP_Adv_Backoff	par défaut : 0 à 3 s	Chaque fois qu'un C_RP_Adv déclenché est envoyé, une nouvelle valeur aléatoire entre 0 et 3 est utilisée

6. Considérations pour la sécurité

6.1 Menaces possibles

Les menaces qui affectent le mécanisme de BSR PIM sont principalement de deux formes : attaques de déni de service (DoS) et attaques de détournement de trafic. Un attaquant qui subvertit le mécanisme de BSR peut empêcher le trafic de diffusion groupée d'atteindre les receveurs prévus, peut détourner le trafic de diffusion groupée sur un endroit d'où il peut le surveiller, et peut éventuellement inonder des tiers avec du trafic.

Le trafic peut être empêché d'atteindre les receveurs prévus par un des deux mécanismes suivants :
- Subvertir un BSM, et spécifier des RP qui ne vont pas réellement transmettre le trafic.

o S'enregistrer auprès du BSR comme C-RP, et ensuite ne pas transmettre le trafic.

Le trafic peut être détourné en un lieu d'où il peut être surveillé par les deux mécanismes ci-dessus ; dans ce cas, les RP vont transmettre le trafic, mais ils sont situés de façon à faciliter la surveillance ou des attaques par interposition sur le trafic de diffusion groupée.

Un tiers peut être inondé par l'un ou l'autre des deux mécanismes ci-dessus en spécifiant le tiers comme RP, et enregistrer que le trafic soit ensuite transmis au tiers.

6.2 Limitation des attaques de DoS de tiers

L'attaque de DoS sur un tiers ci-dessus peut être largement réduite si les routeurs PIM qui agissent comme DR ne continuent pas à transmettre le trafic de Register au RP en présence de réponses ICMP Protocole injoignable ou Hôte injoignable. Si un routeur PIM qui envoie des paquets Register à un RP reçoit une de ces réponses à un paquet de données qu'il a envoyé, il devrait limiter le débit de transmission des futurs paquets Register à ce RP pendant une courte période.

Comme cela n'affecte pas l'interopérabilité, les détails précis sont laissés à la décision des mises en œuvre. Cependant, on note qu'un routeur qui met en œuvre une telle limitation de débit doit seulement le faire si le paquet ICMP fait correctement écho à une partie d'un paquet Register qui a été envoyé au RP. Si cette vérification n'était pas faite, le simple envoi de paquets ICMP "injoignable" au DR avec l'adresse de source du RP usurpé serait suffisante pour causer une attaque de déni de service sur le trafic de diffusion groupée originaire de ce DR.

6.3 Sécurité du message Bootstrap

Si un routeur PIM légitime dans un domaine est compromis, il n'y a rien qu'un mécanisme de sécurité puisse faire pour empêcher ce routeur de subvertir le trafic PIM dans ce domaine.

Les mises en œuvre DEVRAIENT fournir une option de configuration par interface où on puisse spécifier qu'aucun message Bootstrap ne va être envoyé de, ou accepté sur l'interface. Ceci devrait généralement être configuré sur tous les PMBR afin de ne pas recevoir de messages des domaines du voisinage. Cela évite de recevoir des messages legitimes avec des informations de BSR en conflit provenant d'autres domaines, et empêche aussi les attaques de BSR provenant des domaines du voisinage. Cette option est aussi utile sur les interfaces d'extrémités où seuls sont présents des hôtes. Cependant, la section des considérations sur la sécurité de la [RFC4601] déclare qu'il devrait y avoir un mécanisme pour ne pas accepter de messages PIM Hello sur les interfaces d'extrémité et que les messages devraient seulement être acceptés de voisins PIM valides. Il peut cependant y avoir des problèmes supplémentaires avec les messages Bootstrap en envoi individuel ; voir ci-dessous. En plus d'éliminer tous les messages Bootstrap en diffusion groupée sur les PMBR, on recommande aussi de configurer les PMBR (à la fois vers les autres domaines et sur les interfaces d'extrémité) à éliminer tous les messages PIM en envoi individuel (message Bootstrap, annonce de RP candidat, PIM Register, et PIM Register-Stop).

6.3.1 Messages d'amorçage en envoi individuel

Il y a des problèmes de sécurité possibles avec les messages Bootstrap en envoi individuel. Les vérifications de traitement de message Bootstrap empêchent un routeur d'accepter un message Bootstrap provenant de l'extérieur du domaine PIM, car l'adresse de source des messages Bootstrap doit être un voisin PIM immédiat. Il y a cependant une petite fenêtrte de temps après un réamorçage où un routeur PIM va accepter un mauvais message Bootstrap en envoi individuel provenant d'un voisin immédiat, et il serait possible durant cet intervalle d'envoyer un message Bootstrap en envoi individuel à un routeur de l'extérieur du domaine, en utilisant une adresse de source usurpée d'un voisin. La meilleure façon de se protéger contre cela est d'utiliser le mécanisme sus-mentionné de configuration des interfaces de bordure et d'extrémité à éliminer tous les messages Bootstrap, incluant les messages en envoi individuel. Cela peut aussi être empêché si les PMBR effectuent le filtrage d'adresse de source pour empêcher les paquets d'entrer dans le domaine PIM avec des adresses IP de source qui sont des adresses d'infrastructure dans le domaine PIM.

L'utilisation de messages Bootstrap en envoi individuel est seulement pour la rétro compatibilité. Du fait de possibles implications de sécurité, les mises en œuvre qui prennent en charge les messages Bootstrap en envoi individuel DEVRAIENT fournir une option de configuration pour décider si ils sont à utiliser.

6.3.2 Sous réseaux multi-accès

Comme mentionné ci-dessus, les mises en œuvre DEVRAIENT fournir une option de configuration par interface afin que les interfaces d'extrémité et les interfaces vers d'autres domaines puissent être configurées à éliminer tous les messages Bootstrap. Dans ce paragraphe, on va examiner les sous-réseaux multi-accès où il y a plusieurs routeurs PIM dans un domaine PIM et des routeurs PIM en dehors du domaine PIM ou des hôtes qui ne sont pas de confiance. Sur de tels sous-réseaux, on devrait (si possible) configurer les PMBR à éliminer les messages Bootstrap. Ceci est possible pourvu que les routeurs dans le domaine PIM reçoivent les messages Bootstrap sur d'autres sous-réseaux internes. C'est-à-dire, pour chacun des routeurs sur le sous réseau multi-accès qui sont dans notre domaine, l'interface de RPF pour chacune des adresses de candidat BSR doit être une interface interne (une interface qui n'est pas sur un sous-réseau multi-accès). Il y a cependant des topologies de réseau où cela n'est pas possible. Pour de telles topologies, on recommande que l'en-tête d'authentification IPsec (AH, *Authentication Header*) soit utilisé pour protéger la communication entre les routeurs PIM dans le domaine, et que de tels routeurs soient configurés à éliminer et enregistrer les tentatives de communication provenant de tout nœud qui ne réussit pas les vérifications d'authentification. Quand tous les routeurs PIM sont sous le même contrôle administratif, cette authentification peut utiliser un secret partagé configuré. Afin d'empêcher les attaques en répétition, on va avoir besoin d'une association de sécurité (SA) par envoyeur et d'utiliser l'adresse de l'envoyeur pour la recherche de SA. La sécurisation des interactions entre les voisins PIM est discutée plus en détails dans la section des considérations sur la sécurité de la [RFC4601], et on n'en dira pas plus ici. Les mêmes mécanismes de sécurité qui peuvent être utilisés pour sécuriser les messages PIM Join, Prune, et Assert devraient aussi être utilisés pour sécuriser les messages Bootstrap. Comment exactement sécuriser les messages PIM de liaison locale est encore à l'étude dans le groupe de travail PIM ; voir la [RFC5796].

6.4 Sécurité du message Candidate-RP-Advertisement

Même si il n'est pas possible de subvertir les messages Bootstrap, un attaquant pourrait être capable d'effectuer la plupart des mêmes attaques simplement en envoyant des messages C-RP-Adv au BSR en spécifiant le choix de RP de l'attaquant. Donc, il est nécessaire de contrôler l'envoi des messages C-RP-Adv essentiellement de la même façon qu'on contrôle les messages Bootstrap. Cependant, les messages C-RP-Adv sont en envoi individuel et voyagent normalement sur plusieurs bonds, de sorte que leur contrôle est plus difficile.

6.4.1 Sécurité non cryptographique des messages C-RP-Adv

On recommande que les PMBR soient configurés à éliminer les messages C-RP-Adv. On pourrait configurer les PMBR à éliminer tous les messages PIM en envoi individuel (message Bootstrap, annonces de candidat RP, PIM Register, et PIM Register Stop). Les PMBR peuvent aussi effectuer le filtrage d'adresse de source pour empêcher les paquets d'entrer dans le domaine PIM avec des adresses IP de source qui sont des adresses d'infrastructure dans le domaine PIM. On recommande aussi que les mises en œuvre aient un moyen de restreindre de quelles adresses IP le BSR accepte les messages C-RP-Adv. Le BSR peut alors être configuré à seulement accepter les messages C-RP-Adv provenant des adresses d'infrastructure sur le sous réseau utilisé pour les candidats RP.

Si les topologies d'envoi individuel et de diffusion groupée sont connues pour être congruentes, les vérifications suivantes devraient être faites. Sur les interfaces qui sont configurées à être des sous réseaux d'extrémité, tous les messages C-RP-Adv devraient être éliminés. Sur les sous réseaux multi accès avec plusieurs routeurs et hôtes PIM qui ne sont pas de confiance, le routeur peut au moins vérifier que l'adresse de source de contrôle d'accès au support (MAC, *Media Access Control*) est celle d'un voisin PIM valide.

6.4.2 Sécurité cryptographique des messages C-RP-Adv

Pour une vraie sécurité, on recommande que tous les C-RP soient configurés à utiliser l'authentification IPsec. Le processus d'authentification pour un message C-RP-Adv entre un C-RP et le BSR est identique au processus d'authentification pour les messages PIM Register entre un DR et le RP pertinent, sauf qu'il va normalement y avoir moins de C-RP dans un domaine qu'il n'y a de DR, de sorte que la gestion de clé est un peu plus simple. On ne décrit pas plus les détails de ce processus ici, mais se référer à la section des considérations sur la sécurité de la [RFC4601]. Noter que l'utilisation de la sécurité cryptographique pour les messages C-RP-Adv ne supprime pas le besoin de mécanismes non cryptographiques, comme expliqué ci-dessus.

6.5 Déni de service en utilisant IPsec

Un souci supplémentaire est celui des attaques de déni de service causées par l'envoi de forts volumes de messages Bootstrap ou de messages C-RP-Adv avec des informations invalides d'authentification IPsec. Il est possible que ces messages puissent submerger les ressources de CPU du receveur.

Les mécanismes de sécurité non cryptographique ci-dessus restreignent d'où les messages Bootstrap en envoi individuel et les messages C-RP-Adv sont acceptés. De plus, on recommande que des mécanismes de limitation de débit puissent être configurés, à appliquer à réception des paquets PIM en envoi individuel. Le limiteur de débit DOIT limiter en débit indépendamment les différents types de paquets PIM -- par exemple, un flux de messages C-RP-Adv NE DOIT PAS causer l'élimination par le limiteur de débit des messages Bootstrap à faible débit. Un tel limiteur de débit pourrait lui-même être utilisé pour causer une attaque de déni de service en causant l'élimination de paquets valides, mais en pratique ceci va très probablement restreindre les mauvais messages PIM. Le limiteur de débit va empêcher les attaques sur PIM d'affecter les autres activités sur le routeur receveur, comme l'acheminement en envoi individuel.

7. Contributeurs

Bill Fenner, Mark Handley, Roger Kermode et David Thaler ont largement contribué au présent document. Ils ont été les auteurs de ce document jusqu'à la version 03, et la plus grande partie du texte actuel provient de la version 03.

8. Remerciements

PIM-SM a été conçu depuis de nombreuses années en empruntant les idées d'un large groupe de personnes, parmi lesquelles Deborah Estrin, Dino Farinacci, Ahmed Helmy, Steve Deering, Van Jacobson, C. Liu, Puneet Sharma, Liming Wei, Tom Pusateri, Tony Ballardie, Scott Brim, Jon Crowcroft, Paul Francis, Joel Halpern, Horst Hodel, Polly Huang, Stephen Ostrowski, Lixia Zhang, Girish Chandranmenon, Pavlin Radoslavov, John Zwiebel, Isidor Kouvelas et Hugh Holbrook. La présente spécification de BSR tire une grande partie de son texte de la RFC 2362.
De nombreux membres du groupe de travail PIM ont contribué par des commentaires et des corrections au présent document, au nombre desquelles on retiendra particulièrement Christopher Thomas Brown, Ardas Cilingiroglu, Murthy Esakonu, Venugopal Hemige, Prashant Jhingran, Rishabh Parekh et Katta Sambasivarao.

9. Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2365] D. Meyer, "Diffusion groupée sur IP limitée administrativement", juillet 1998. (BCP0023)

[RFC4007] S. Deering et autres, "Architecture d'adresse IPv6 calibrée", mars 2005. *(P.S.) (MàJ par* RFC7346)

[RFC4291] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", février 2006. (*MàJ par* 5952 et 6052, 8064) *(D.S.)*

[RFC4601] B. Fenner et autres, "Diffusion groupée indépendante du protocole - Mode épars (PIM-SM) : spécification du protocole (révisée)", août 2006. (*Remplace* RFC2362) (*MàJ par* RFC5059 ; *Remplacée par* RFC7761, STD83) *(P.S.)*

[RFC5015] M. Handley et autres, "Diffusion groupée bidirectionnelle indépendante du protocole (BIDIR-PIM)", octobre 2007. *(P.S.)*

10. Références pour information

[RFC2362] D. Estrin et autres, "Mode épars de diffusion groupée indépendante du protocole (PIM-SM) : Spécification du protocole", juin 1998. *(Obsolète, voir* RFC4601, RFC5059)

[RFC3446] D. Kim et autres, "Mécanisme de point de rendez-vous (RP) en envoi à la cantonade utilisant la diffusion groupée indépendante du protocole (PIM) et le protocole de découverte de source de diffusion groupée (MSDP)", janvier 2003. *(Info.)*

[RFC4610] D. Farinacci, Y. Cai, "Point de rendez-vous d'envoi à la cantonade utilisant la diffusion groupée indépendante du protocole (PIM)", août 2006. *(P.S.)*

[RFC5796] W. Atwood, S. Islam, M. Siami, "Authentification et confidentialité dans les messages de liaison locale du mode de diffusion groupée éparse indépendante du protocole (PIM-SM)", mars 2010. (*MàJ* RFC4601). *(P.S.)*

[IANA] IANA, <http://www.iana.org/assignments/address-family-numbers>.

Adresse des auteurs

Nidhi Bhaskar
Arastra, Inc.
P.O. Box 10905
Palo Alto, CA 94303
USA
mél : nidhi@arastra.com

Alexander Gall
SWITCH
P.O. Box
CH-8021 Zurich
Switzerland
mél : alexander.gall@switch.ch

James Lingard
Arastra, Inc.
P.O. Box 10905
Palo Alto, CA 94303
USA
mél : jchl@arastra.com

Stig Venaas
UNINETT
NO-7465 Trondheim
Norway
mél : venaas@uninett.no

Déclaration complète de droits de reproduction